Department of Homeland Security
Data Privacy and Integrity Advisory Committee

OFFICIAL MEETING MINUTES

Tuesday, December 6, 2005
J. W. Marriott Hotel
Capitol Ballroom (E&F)
1331 Pennsylvania Avenue NW
Washington, DC 20004

AFTERNOON SESSION

Ms. Sotto: I would like to call to order the afternoon session of the DHS Data Privacy and Integrity Advisory Committee. Our next panel is seated. Thank you. Our next panel will address, redress which is probably collectively, if we had to choose a topic, the most interesting topic to this group and one that we're most concerned about. So we very much appreciate your sharing of thoughts and ideas with us. Our first panelist is Jim Kennedy. Jim is the Director for the office of Transportation Security Redress, reporting to the special counselor. Mr. Kennedy joined TSA in September 2003 as a Program Manager with the Office of Information Technology. Previously, Mr. Kennedy has held positions as special assistant to the Chief of Staff and special assistant to the chief operating officer. He was a key contributor to the strategic direction of OTSR during its start up phase. Thank you Mr. Kennedy.

REDRESS AT DEPARTMENT OF HOMELAND SECURITY

Mr. Kennedy: Good afternoon. Before I begin, I would like to thank you for giving me the opportunity to discuss redress efforts at the Transportation Security Administration. As some of you know, TSA is just now completing its reorganization efforts after the new director, Mr. Hawley, was sworn in. As a part of that process, I was named director of the office of Transportation Security Redress about a little bit over two weeks ago. But as you said, madam chairperson, I am very familiar with the redress efforts from my position as the special assistant to the Chief of Staff for TSA. As all of you know, TSA was created as a part of the Aviation and Transportation Security Act in the wake of 9/11. Its mission is to protect the nation's transportation systems by insuring the

freedom of movement for people and commerce. In support of that mission, TSA works with various law enforcement and intelligence agencies to identify individuals who currently or could potentially pose a threat to any mode of transportation. As you know, TSA has instituted a number of directive centers designed to prevent these individuals from achieving their goals. Unfortunately, there are instances where innocent people are misidentified as someone who poses a security threat. We recognize that we have an obligation to correct that problem. To fulfill the obligation, Congress has passed the Intelligence Reform Act that required TSA to create the Office of Redress. At TSA, the definition of redress is simple. It is the process by which an individual who has been identified as a threat, either correctly or incorrectly, can appeal that determination and correct erroneous information. The mission of TSA's Redress Office is to support the standardized processes that are in place to do just that. The Redress Office is separate from the program offices that have responsibility for determining threats to transportation. To avoid any potential conflicts of interest, the director of the Redress Office reports to the Special Counselor of TSA who, in turn, reports to the assistant secretary. At TSA, we offer redress for two different types of programs, exercise of right or what we term freedom of movement, and application for right benefit or privilege such as licenses and work privileges. I would like to take a moment to highlight the redress processes for each category that are currently in place at TSA. First off is exercise of right. When an individual has been subjected to repeated delays while traveling through our nation's airport, they're told that the delay could be a result of being misidentified for an individual on a watch list. They're given instructions on how to contact TSA Headquarters for redress relief. When the person calls our TSA Contact Center or logs into our web site, they're given the opportunity to participate in our watch list clearance protocol otherwise known as our passenger identity verification. If the person wants to participate, they're asked to submit a PIVF or Passenger Identity Verification Form along with re-notarized or certified documents that verify the individual's identity. Once information is received, TSA compares the information against the watch list. If we conclude that the individual seeking redress is not on the watch list, we notify any appropriate parties, including the airlines, in an effort to try and streamline the clearance process for the individual. If we cannot distinguish the individual seeking redress from a person on the watch list, then we will work with the Terrorist Screening Center Redress Office to make an initial determination. If the determination is not favorable, we will inform the requester that we're unable to author redress at the time, at this time. So far, over 30,000 members of the traveling public have submitted PIVF paperwork and have received relief from the Office of Redress since its inception in November of `04. It is important to note that TSA is developing other programs such as Secure Flight, which I believe you've been briefed on, that are designed to minimize the number of instances where people are misidentified as potential terrorist threats. The second type of redress that we offer is application, redress for application of right benefit or privilege. There are

security directives in place that require companies to give, to get TSA approval prior to hiring individuals for certain jobs, such as truck drivers transporting hazardous materials. If TSA, in consultation with other law enforcement and intelligence agencies, make a determination that the individual seeking clearance is a potential threat, it will deny approval for the license or the employment. In both of these instances, the determination is known as the initial agency decision. If an individual would like to appeal the TSA decision, there is a process in place to do so. In all cases, individuals applying for redress are notified that the personal information they submit to TSA for evaluation is covered by federal privacy laws and is handled as such. TSA only collects information it needs that is relevant to sufficiently adjudicate redress claims. The disclosure of the information is limited to those DHS personnel, law enforcement or intelligence agencies who have a need to know in order to perform their official duties related to redress. In addition, TSA personnel handling the personal information must have completed the privacy training mandatory for all TSA employees prior to working in the Redress Office. Lastly, after the final decision is issued on an individual's redress request, the requester's information is stored according to TSA policy for sensitive but unclassified material. We are currently working with the appropriate parties within TSA to develop a records disposition schedule. Thank you for your time and attention. I'll be happy to answer any questions that you may have.

Ms. Sotto: This is going to be fun. Thank you very much Mr. Kennedy. Let's start with Howard Beales.

Mr. Beales: You mentioned there are about 30,000 people who have submitted paperwork and received relief. How many people submitted paperwork and were denied because they could not be distinguished from somebody on the list?

Mr. Kennedy: Right now I think that number -. It's a very low number. It's -. I do believe the number is around 60. That is what I know at this time. And those people were actually -. We did not make the determination by ourselves. We did work in conjunction with the Terrorist Screening Center. I will be happy to go back and get the exact figure, but I think it is 60.

Mr. Beales: I would appreciate knowing the exact figure. That would be wonderful. Do you know if these were people that were, and maybe there's not a difference here -. Is there a distinction between people who were, in fact, on the list and people who we just couldn't distinguish from somebody who is on the list?

Mr. Kennedy: No. They were people who were selectees. They were not people who were no-flys or people who were selectees. And in that case, the people were allowed to fly. Obviously they just had to go through additional screening. So we've not received anybody who was actually on the no-fly list.

Ms. Sotto: Joanne McNabb.

Ms. McNabb: You said that when you cleared somebody, a false positive, I assume is what you mean, that you would share that information or that pact with other parties including the airlines. What kind of information, personal information, do you share with the airlines in that case?

Mr. Kennedy: Well, actually the airlines have the watch list, and there's a specific section of the watch list that talks about the individuals. And the information that is on that list is usually their name, their date of birth and their address.

Ms. McNabb: Of the cleared person, indicating that it is a cleared person?

Mr. Kennedy: Correct.

Ms. McNabb: Well, actually that was my other question is, what modification might be made in the watch list when you've cleared somebody as being a false positive?

Mr. Kennedy: That's it, and the list is actually transmitted to the airlines once every 24 hours. And so once a person gets on the list, it is updated and sent to the airlines within 24 hours.

Ms. McNabb: Thank you.

Ms. Sotto: Mr. Wright.

Mr. Wright: What's the average time frame for making these types of decisions and not only the average time frame but, let's say, in the longest time frame that someone has been in limbo, not knowing?

Mr. Kennedy: We advertise that the average time frame is between 45 and 60 days. There have been cases in the past where it's taken longer because of the fact we've not been able to make a determination. I do not know what the longest time has been. I just don't know that information. But on average, if it is something, if it is someone that we can clear right away, once we get the information into our office, we are able to check it. We're able to put that person on the cleared list and have it updated with that next cycle, the 24-hour cycle. So it just depends on when we get the paperwork, if it is correct. With the notarized or certified copies, we can turn that around extremely quickly, but we do say from the time that the individual mails the information to until the time that the information is updated on the cleared list can be 45 to 60 days. We're actually, obviously, working on trying to reduce that, but that is what the standard is right now.

Ms. Sotto: Mr. Sheehan.

Mr. Sheehan: Let me get a little more granular and see if I misunderstood some of the terms. Thirty thousand people saw some sort of redress since 11 of `04.

Mr. Kennedy: Correct.

Mr. Sheehan: What did the number 60 describe?

Mr. Kennedy: That described the people who, and this is what I'm going to get the exact number, but it described the people who we were unable to offer redress because of the fact that that person may have, was actually somebody that we were actually looking for.

Mr. Sheehan: Okay. Using your numbers then, 29,940 people got some sort of redress.

Mr. Kennedy: Correct.

Mr. Sheehan: By that do we mean that they were removed the next time from, removed from the list and didn't have to suffer any delay?

Mr. Kennedy: What it means is those individuals were placed on the cleared list, and when we -. Before we start the PIVF process with anyone, it is stated up front that what this will do will be to place your name on the cleared list. It will not, quote unquote, remove you from the list because of the fact that the person that we are still looking for is out there. What it essentially means is as long as you are an active member of the cleared list, you will actually have to -. Instead of being allowed to go to the kiosk, you will actually have to go up to the ticket counter and then the individual at the ticket counter, you will notify them that you're on the cleared list. They'll check the cleared list and that's it. Unfortunately, that is the system we have right now.

Mr. Sheehan: Did the fact that out of 30,000 people 60 couldn't be determined, and 29,940 were put on the cleared list, did that instruct you or teach your organization anything about, perhaps, the over breadth of the list to start with?

Mr. Kennedy: That is a question, unfortunately, I do have to -. It taught us something, that yes, that is something we need to take a look at. And it also has taught the various administrators we've had that it's something we need to take a look at between Mr. Stone and now

Mr. Hawley, and that is something we have looked at. But that is, of course, that's outside the realm of redress.

Mr. Sheehan: Thank you.

Ms. Sotto: I did, by the way, figure out the blind spot that is those two. So you were right. There is a blind spot. Mr. Alhadeff.

Mr. Alhadeff: Thank you. I actually had a couple of questions based on the statements, and please feel free to correct me if I mistook a note because, on this one, I want to be fairly specific. I think that you had said that if a person has been inconvenienced by repeated delays, they have an opportunity to participate. I would

think that if you were inconvenienced by one delay, you should have an opportunity to participate because clearly you've been a false positive once. If you need to be a false positive multiple times, I don't really think I understand that concept. And the other thing that comes up is in our paper, we pointed out there are problematic names, like you might have a person whose name is Leslie James. It could be a man. It could be a woman. One name could be the first name. Both names could be the first name.

Those are really the kind of a lot of the problematic names, and it would strike me that if in the watch list, we have someone who is a Leslie James who's a person who we believe to be a male 30-some odd years of age, and the person who presents themselves is an 18-year-old woman. I'm not exactly sure why we need to have her fill out a PIVF and get three forms of notarized identification because clearly, that is not the person you're looking for absent a lot of expensive surgery. And then the last question I had is when the cleared list might get to 50,000, what is the process by which a person finds a name on the cleared list? Is that a computer-generated search that goes on that list? Because I can't imagine someone's going to be rifling through 50,000 names in order to find the right one.

Mr. Kennedy: I will try and answer your questions in order. Instead of why is it that a person is not offered redress if they're impacted once, there are actually more reasons that a person will be selected for additional screening other than if somebody is on the watch list. There are other screening procedures that are in place. Some are random. Some are if there are different profiles, for example, that a person will fit, and when we say repeated issues or repeatedly impacted, that is usually a sign to us that it's a watch list issue versus a random selection. So that's why we say random versus one time. And that is to make sure that it is not another category that you're falling in. This is actually the watch list piece.

Mr. Alhadeff: Let me follow up on that piece, but you guys or the people on the line who are doing the choice -. I mean, I've bought the one- way ticket before, and I've gotten the nice interaction. And by the way, they're very polite now, so thank you. And I understand that there are different reasons for which you should be screening including just pure random, your X number the computer generated, you saw the S on your ticket. Thank you, you're going to get screening. But I would assume you know when somebody's being screened because they might be a match versus when somebody's being screened because they're randomly generated. And therefore, if someone is being screened because there's a match, and it turns out they're false positive, I would think at some point you would be able to give that person relief a little faster because obviously, the frustration with the system comes from the people who are stuck in the system more often.

Mr. Kennedy: And you're kind of assuming that we are -. One of the things that I wanted to say in follow up to your other questions, but it really applies here, is the list

itself is transmitted to the airlines in its entirety, and the airlines actually use their system to determine if a person should be stopped or if it may be a match with someone on the actual, the watch list. It could be airline A may look at first initial, last name. Airline B may look at full name, first and last name. That's one of the reasons why. I believe you've gotten a briefing on Secure Flight. That's one of the reasons for Secure Flight, so we can cut down on the misidentified persons in this case as well at the time something happens. In the Redress Office, I don't know why that person was stopped. If that person says that they were impacted, we usually ask is it once, or if it's more than once, if it's once, what we want to do before going through all of this, we want to say, Okay, let's make sure that this is the actual problem so we can say, Okay, this is going to help who is just random and you have it one time. Then this is not going to do you any good, and you're just turning in your information, so that's really why we want to do that. And your third question, I'm sorry. We kind of got into the discussions. I've forgotten your third question.

Mr. Alhadeff: Two and three were the Leslie James. Do you really have to turn in the PIVF if the person is obviously not the person you're looking for? And the last one was, is the list mechanical or is it something that is searchable so you get a quick return on the query of is this person the same person?

Mr. Kennedy: The answer to your third question, it depends on the airline system. It is transmitted in its entirety. Like I said, every 24 hours to the airlines, it's how they input it and how they use it in their systems is what determines it. And as for Leslie James, we put out to the airlines the description of the individual that we're looking for. Again, it's what the airlines give to, make available to the ticketing agent as to whether that person will be selectively screened or if they do so, how they really address that, but we give the information to them.

Ms. Sotto: Thank you very much. Mr. Sabo.

Mr. Sabo: Just briefly for everybody on the committee, could you just briefly indicate what is the selectee list, these of the, the watch list, and then I have a question.

Mr. Kennedy: Well, it's all one list. It is called a Federal Watch List. There are two components. One is a selectee list, and the other one is a no-fly list. A selectee list is a list in which you are allowed to fly, but you're subjected to secondary screening, additional screening. A no-fly list is just that you do not fly. You can change to a different airline. You can do whatever you want to. All airlines have the same information, and the government has made the determination that you're not allowed to fly at this time. So those are two lists, and together they're called the watch lists.

Mr. Sabo: With respect to those who are not allowed to fly with extra screening, just a category, if they show up at the airport, do they automatically receive or have an

encounter with a federal official at the airport, or do they typically -. I guess I'm getting to of the 30,000 who have requested redress or 30,000 of which 60 were denied, do you have any sense of the percentage or hit against the no-fly list, these of the selectee list? And the reason I get to that is the obvious one of if they're going to encounter or have to discuss this with a federal official and seek redress. That could be the opportunity to have them show their documentation to that official and avoid the weeks of waiting while they go through a process of notarization and so on. Anyway, it's sort of a cascading question, but if you can follow it.

Mr. Kennedy: To answer your question, the individuals who have been, who have submitted for redress, those that we have not been able to offer redress because they were found to be - we could not distinguish them from someone on the watch list or people who were actually selectees, not no-flies. To answer your no-fly question, I can't really -. I do know that they have an encounter of some sort. I don't know what that encounter is.

Mr. Sabo: Again, the follow up would be - if you could again - the problem would be time, but I guess for a passenger who may have been multiple, over multiple occasions stopped for additional screening or whatever, as you look forward to Secure Flight in the future, once the program is introduced, are you looking at ways to speed up the ability of passengers to get on a cleared list such as at an airport, meeting with a federal official, showing credentials and then having them process immediately or to initiate the processing, you still probably have to do a check, but it would just seem to me that's a lot more convenient than having them wait to go back home and then to go to a notary and the whole process of notarization, as we all know, is not foolproof. And therefore, showing it to a federal official would be just as adequate as or better than having a notary look at the credentials. Have you thought of about that type of process for Secure Flight?

Mr. Kennedy: Well first of all, I don't run Secure Flight, but from the Office of Redress, we're actually looking at multiple ways right now. But again, since I've been on board for about two weeks, I've not had a chance to do that, no.

Ms. Sotto: I'm going to give the last question to Howard Beales. I owe you one because Howard's been working on this so heavily.

Mr. Beales: I just wanted to follow up. You said that you give the airline the physical description information about people who are on the list. I guess I'd been under the impression that the only information on the list was name and date of birth.

Mr. Kennedy: That's when we said the cleared list, but there's other information that is given on the selectee on the other portion of the watch list.

Mr. Beales: On the selectee portion of the watch list?

Mr. Kennedy: Other portions of the watch list, yes. The cleared section, we're saying name and date of birth. On the other portions of the watch list, which is selectee and no-fly, I do believe they're given additional information.

Mr. Beales: Okay. Do you know what that information is?

Mr. Kennedy: No, I do not.

Mr. Beales: Thank you.

Ms. Sotto: Mr. Kennedy, I'm fairly certain we're going to have follow-up questions for you.

Mr. Kennedy: That's fine.

Ms. Sotto: If you wouldn't mind if we follow up with questions to you, and if you could provide responses, we would very much appreciate that.

Mr. Kennedy: Please do.

Ms. Sotto: Our next witness is Caroline Hunter. Ms. Hunter currently serves as executive director to the Citizenship and Immigration Services Ombudsman. Previously, Ms. Hunter was Deputy Counsel to the Republican National Committee where she counseled the RNC and state parties on the Help America Vote Act of 2002. Thank you, and welcome.

Ms. Hunter: Thank you, and thank you for the kind invitation to join the committee this afternoon. I'm here on behalf of Patosh Khoudry, who was appointed the first CIS Ombudsman, that is, Citizenship and Immigration Services Ombudsman. He was appointed in June 2003. He's actually traveling this week, meeting with different employer organizations and community-based organizations, which our office does a lot of. And as you may know, our office was created by the Homeland Security Act of 2002. The mission of the office is to assist individuals and employers in resolving problems that they may be having with USCIS and to identify areas in which they're having the problems and to the extent possible, propose recommendations on how USCIS might be able to better their practices to eliminate these problems that individuals are having. Our offices take a little bit of a different approach, I think, to redress in particular, and that is because our office only has approximately 24 people. And as you may know, USCIS handles hundreds of thousands of customer inquiries and complaints per month. So with that in mind, we only have 24 people so we're not able, obviously, to answer everybody's question about their immigration case. So what we have done is we've tried to focus on some of the more egregious cases where people have taken a significant amount of time in order to get their immigration benefit, or they're just unable to use the regular USCIS process for whatever reason. And so we try to assist those people who have the egregious problems. In addition, the primary tact we have taken in our office is to study the

complaints that we receive and to study the systemic problems that may be going on at USCIS and propose, recommend, excuse me, to recommend changes to them. That, in our view, would clean up the process and eliminate many of the problems that individuals are having. So we're taking a more holistic approach to redress at this point, and that's all I have.

Ms. Sotto: Thank you. Any questions? Ramon, why don't you go ahead and ask Mr. Kennedy your question from earlier.

Mr. Barquin: First of all, I think a lot of the questions we're really looking for statistics to tie back to the efficiency of the processes, but I had a specific question because all of the redress that you mentioned basically dealt with getting off the list and getting onto the cleared list. On the other hand, there must have been a number of situations where, as a result of one or multiple false positives, people missed flights and had substantial not just inconvenience but damages, and are there any court challenges? First of all, is there any process for redress where there has been harm beyond just inconvenience? And second, are there some court challenges of this, of the redress, currently that you're aware of?

Mr. Kennedy: Not that I'm aware of. In my short time, I've not run across any challenges. Even the time before as special assistant, I did not recall any court challenges. Most of the redresses, redress claims that we get in the office are because people have been impacted in the airport, and they're seeking redress to speed up the time in which they can get to their flights.

Mr. Barquin: Do you have any statistics as to number of people who actually missed flights as a result of added screening?

Mr. Kennedy: Our office doesn't keep that. It may be kept in another part of TSA, but I don't see it, and I don't have any of the statistics, no.

Ms. Sotto: Jim, did you have a question from earlier?

Mr. Sheehah: Yes, I do. It's a quick one, and you may not know this. How far down in the airline industry does the dissemination of the list go? For example, if I had a charter service and I had six ten-passenger planes that I chartered and I took people on, would I get the list?

Mr. Kennedy: I don't know. I do not know.

Mr. Sheehan: Thank you.

Ms. Sotto: Joe Leo.

Mr. Leo: Yes. Ms. Hunter, I've made several comments on the data integrity side of our committee's work. Specifically, through other reports rather than personal

experience, there have been some comments not very complimentary about CIS's database and the accuracy of their databases. As your office deals with problems and complaints, could you elaborate a little on what CIS may be doing about this, number one, how much a percentage or what may your office solve in terms of correcting data that was wrongly inputted or wrongly given or whatever and what steps you're recommending in a holistic manner that might help improve the overall quality and, therefore, reduce the number of potential complaints because of the data integrity of the data holdings within CIS.

Ms. Hunter: That's definitely a problem, and our office has been looking into those types of areas in particular. We believe the best approach, and I think USCIS would agree with this, and they're pushing to do this as we speak, is to have one computer system and so that all of the databases speak to one another. At this point, there are several different databases within USCIS and, unfortunately, just because one is information may be updated in one system, that doesn't mean it's necessarily been updated in another. So that's an enormous problem that DHS is fully aware of, and again, is hoping to have a completely new computer system that would solve a lot of those problems. In the short term, we're looking for smaller problems that, for example, the change of address issue when an applicant changes their address, they have to send the new address into a couple of places and unfortunately, the information isn't always passed along as I said earlier. So we're looking at ways where that might become a more efficient process, at least in the short term.

Mr. Leo: The reason I've asked that was in another direction is that we have visited several, we'll just call them screening offices, one at TSA and so forth and CBP Customs and Border Protection, and they list the databases, and of course one of them is CIS, and as you can see, the government starts aggregating databases, how important the data integrity issue becomes. So you're part of that network, and that's why I raised today the integrity question in that context as well.

Ms. Sotto: Mr. Alhadeff.

Mr. Alhadeff: Thank you. I actually had a question which was asking if you could elaborate -. In the report, they talk about some of the economic impact issues that result when businesses or universities have interruptions of people that are coming over for conferences or to do business. Can you address things that are being done to kind of address those impacts and perhaps minimize some of the burdens that those people feel they have as they try to enter the country?

Ms. Hunter: Well, that problem is widespread. It is in various different parts of immigration benefits process. In other words, sometimes those people are affected through the non-immigrant applications and sometimes through the immigrant applications. In your case, I recommend that approach which is spelled out in the annual

report which was submitted to Congress in June of this year, is to completely revamp the process, and that would be for all different applications. And our proposal was to have what we call an up-front process whereby individuals would apply, and the application would be given a more thorough look than is currently done. And I would be able to answer to whether or not you're really potentially a possible applicant. In other words, I would look at more than did you submit the proper fee and did you give me just the exact form and sign it, which is essentially all that is looked at right now. So I would do a more thorough look of your application, and if you don't have all of the proper documentation, I would let you know immediately whereas now you might turn in your application, and they may decide there's not enough information there, but by the time they ask you for more information, it's been a significant period of time. And so that is our recommended approach, sort of holistically, to some of those problems. And what that would do, of course, is speed up the benefits process and make it more customer-friendly.

Mr. Alhadeff: If I could just follow on with one brief -. I mean, it seems like, in some cases, some of this is taken care of through counselor offices when you have, in the non-immigrant situation, people who are making the visa request, and it seems that some countries specifically have tremendous backlogs that don't seem to have really any relationship with whether or not your form was complete. So I guess I'm trying to figure out what is being done to address those concepts because those concepts isn't a question of did you fill out the paperwork correctly, but there's obviously something in the vetting process that's taking a long time.

Ms. Hunter: Actually, a lot of the hold up is people didn't submit enough documentation, and by the time there's a request sent out for more information, by the time the person sends it in, that does slow up the process significantly. Of course, there are other reasons that this process is slow and as you know, a lot of those procedures are done by the department of state on the visa or counselor processing. So the department is working with the department of state as well.

Ms. Sotto: Okay. Joanne McNabb, then John Sabo please.

Ms. McNabb: Ms. Hunter, I'm with the California Office of Privacy Protection. One of the things that we do is we assist people who contact us with resolving privacy problems that they may be having, and one thing that we hear a lot about is people who report that someone else, often enough they believe, a non-citizen is working using the person who contacts us who is using that person's social security number. Is there anything that you do in that area that would - can you help any of these people because, I'm telling you, IRS and Social Security can't?

Ms. Hunter: To be honest, we have not tackled that situation. As you suggested, involves several different entities, and our primary focus right now is focusing on USCIS

and their procedures, so we've not delved into that area as of yet. We hope to in the future.

Mr. Sabo: Just a quick question. I know you mentioned you were, you're studying the complaints you receive overall, and I think you said you were looking at ways to address redress on those complaints. Do you have like a strategy or plan in place to do that? In other words, are you kind of collecting data now, and then you're going to put together a program and look at the top five issues and so on, or have you made decisions about the issue, the severity of the issues and the kind of redress? In other words, is this a structured plan to examine the issues that are raised and to provide new forms of redress, or is it just ad hoc?

Ms. Hunter: Are talking about the specific individuals or the strategy to address a larger problem?

Mr. Sabo: I think it's a larger problem. I think I understood you were saying your strategy was to gather the complaints, study them and examine them, and then determine the best ways to offer redress. I'm just wondering if that's a plan that you will announce in 30 to 60 days or half a year, that you've identified a way to do that in a restructured manner.

Ms. Hunter: We have been operating under a plan, and the way of determining that is to study the pieces that we think will have the broadest impact. So that's essentially the plan, and our annual report spells out some of those areas we've identified as the ones we believe are the most problematic that will help the most people.

Ms. Sotto: Thank you very much for providing a copy of your report to the committee. I'm sure this is also publicly available.

Ms. Hunter: Yes, it is.

Ms. Sotto: Well, we appreciate it, and we will certainly take a look at it. Thank you. I would like to turn to - I'm sorry, I didn't see your tent up. Let's turn to Sandra Bell. Ms. Bell serves as deputy assistant commissioner for the Office of Regulations and Rulings. Ms. Bell provides executive leadership to five divisions in ORR in management of the Customs Ruling Program, civil administrative enforcement programs, regulatory and information law and legal decisions related to navigation and border security issues administered by Customs and Border Protection. Previously, Ms. Bell served as the director of International Trade Compliance for the Office of Regulations and Rulings. Thank you, and welcome.

Ms. Bell: Thank you. Good afternoon. It is a pleasure, and I'm honored to be able to address you. First, I want to just make sure you've paid attention to my bio, that I'm not from the Operational Office, I'm from the Legal Office, so our role in connection with redress issues is entirely different from what you might have heard previously. Redress

and general customs and previously customs and previously, the customs service has been providing redress for over 20 years, probably since the enactment of the Privacy Act and the Freedom of Information Act back in the mid-70's through to all persons who are crossing US borders by air, sea, land and also today's environment, between the borders. As you know, our primary mission is to prevent terrorism at the border, but that primary goal is parallel to the goal of facilitating lawful trade and travel, so we actually look at redress as enhancing our ability to meet the twin goals of providing security while facilitating lawful travel.

Basically, redress provides members of the public a way to help us correct erroneous information in our databases, and in that way, the public can receive more expeditious treatment at our ports of entry. It also helps us to effectuate risk management principles in border security measures as the border enforcement agency, charged generally with providing protection of our borders and preventing terrorism at our borders. Redress procedures, ultimately, help us to focus on the truly high- risk travelers or passengers or persons coming over the borders. As part of our mission to protect the borders by preventing terrorists and terrorist weapons from entering into the country, we have a variety of tools to expedite clearance.

The principle tool for clearing persons at the border is the inter-agency border inspection system. You might have heard about that. It's called IBIS. IBIS resides in what we call ancient TEC system, the Treasury Enforcement Communication Systems, and through this system, we have 24,000+ computer access to our field officers for the purposes of looking and assessing whether or not a person arriving at the border or if people who are arriving through the borders are high risk. IBIS provides law enforcement community with access to the computer, to the computer base enforcement files of the FBI as well and NCIC, the National Crimes Information Center as well as the National Law Enforcement Telecommunication Center. Now because of the way we're structured, CBP - Customs and Border Protection - provides redress through a variety of ways. The principle redress procedures are housed in our Customer Satisfaction Unit which is in our Office of Field Operations which is the largest office within Customs and Border Protection, 22,000+ employees. And basically, for anybody having a problem about why they were stopped, why they were subject to secondary inspection, intensive examination, the redress procedure is simple. Just write a letter to Customer Satisfaction Unit. The address is 1300 Pennsylvania Avenue, 5.5C is the room number - our zip code is 20229. You can also fax us. This is all posted on our web site. The fax number is 202-344-2791.

As I said earlier, that is the primary way redress issues are dealt with in Customs and Border Protection because most of them go through the Office of Field Operations,

our largest office, and that's because the Office of Field Operations is responsible for controlling a lot of the information systems like I mentioned, IBIS, TECS, NAILS.

As a result of our transition into DHS we are now having a lot of the immigration issues included in the Office of Field Operations. NAILS, the National Automated Information Lookout System, is the former Immigration Naturalization Service now incorporated into TECS and IBIS. NIIS, this is the Non- Immigrant Information System. The I-94 is housed there.

We had something long before being brought into the Department of Homeland Security that was called Free and Secure Trade. This was an inter-agency agreement we had with Canada to vet what we call trusted travelers or trusted carriers through a vetting system. Their arrival and departure from the US would be expedited. All of the trusted traveler programs are administered by the Office of Field Operations: NEXUS, SENTRI, what's called PAL, the Pre-enrolled Access Lane. And that information, the information contained in those systems, are handled by the Customer Satisfaction Unit to the extent someone is questioning why they have been kicked out or they're not accepted into one of those trusted traveler programs.

Our next largest office, the Office of Border Patrol, has like 11,000+ employees, and the redress system is handled through two ways. To the extent that the issue involves a person inquiring as a result of information that is contained in the TECS or IBIS system, that complaint or that redress issue is sent to the Customer Satisfaction Unit, the same address I just gave you. To the extent it's a question related to the Alien file, that is handled with a FOIA request, and it's sent to the Citizens and Immigration Services Agency, which currently still processes all the FOIA requests for the Office of Border Patrol. And when we think about the Office of Border Patrol, redress is somewhat a little bit tricky because most of their actions, I would say pretty much all of their actions would involve a situation where they're dealing with potential violators because they're dealing with protecting our borders between the ports of entry, and there is no legal entry of anybody, even US citizens, between the ports of entry.

Other areas outside of law enforcement, the Office of Human Resources Management, which is the HRM Office, handles it a little bit differently. They handle redress issues to the extent someone is questioning why they were not accepted for employment, an employee asking about an application they filed for a promotion. That can be handled under the Privacy Act. And to the extent that there is incorrect information, a correction to the person's record, an amendment can be made. And to the extent they're not satisfied or to the extent we don't agree with them, of course they can go through the judicial process and request expungement. All other inquiries, such as someone asking about why they're being subject to some disciplinary action, that is treated as a FOIA. So in that office, the redress procedures take the form of a FOIA

request or treating their inquiry about what has happened as a FOIA request or Privacy Act request.

And the same thing goes for our Office of Management, Integrity and Inspections, which is the new name for what used to be the Office of Internal Affairs which handled all the in-house disciplinary proceedings. Now that's a little different. They treat all of the requests there as a FOIA request and any inquiries regarding questions as to what is going on, because all of that information, regardless of whether or not the person is subject to the Privacy Act, would be exempt from the access provisions under the Privacy Act.

In a typical redress letter, and I will just take the time to read it, to the extent it goes through the Customer Satisfaction Unit, which receives the bulk of it. And normally in a situation where there is no error that needs to be corrected, the person is just concerned about the fact that they're being stopped. We normally just reply by explaining the fact that in the wake of 9/11, a lot of people are being stopped more than usual, and we just request that they be patient, notifying them of the fact that CBP has the right to subject any international traveler to inspection, so it's not something that is considered to be unusual, and basically letting them know that we try to be as polite and accommodating as possible. And to the extent that they have any questions, to come back, and we'll address it again at an appellate level. The other thing is, to the extent that the information is erroneous, we're happy to find out about it.

As I mentioned earlier, that helps us to provide effective risk management. It also helps us to facilitate lawful travel so that correct information is amended to the record. To the extent it's an automated or electronic system, there are some rules about whether or not you can take something out because it actually affects the audit trail. So what happens is the corrected information is noted in the file, but sometimes the incorrect information is still there. And as I mentioned earlier, the Privacy Act only protects you as citizens and permanent legal residents. To the extent someone is seeking redress under the Privacy Act and they meet that criteria, they can request that the record be amended as I mentioned, but that's usually in a court anyway. To the extent they disagree because it's not a factual issue, it's an opinion, then they can seek judicial review and get expungement, and of course, that's does not apply to non-US citizens or non-permanent residents. The Office of Regulations and Rulings, which is the office where I'm deputy assistant commissioner, recently reorganized, and we now have, to help us to help the agency meet its Privacy Act responsibilities as well as to maybe coordinate the redress responsibilities, a new unit in my office, and there's a new division called Regulations and Disclosure Law Division, and in that division, there is a branch specifically devoted to privacy issues called the Privacy Act Policies and Procedures Branch, and Laurence Castelli, who is here this afternoon, is the chief of that branch. And with that, I'll close.

And to the extent you get too technical in your questions, I reserve the right to defer to Larry. Thank you.

Ms. Sotto: Thank you very much. I have a quick question, and then I'll turn to others. The only information we could find on the web site for redress for CBP was on FOIA. There didn't seem to be, at least readily identifiable, anything on the Customer Satisfaction Unit. Could you comment on that please?

Ms. Bell: My understanding is that it was on the web site. I will have to find out where exactly it is and get back to the committee.

Ms. Sotto: That would be great. If you could follow up in writing, we would appreciate it. Thank you. Howard Beales.

Mr. Beales: Do you have a Privacy Act notice on the I-94 forms, and do you plan to do one?

Ms. Bell: The I-94, I tell you the truth. I really thought that was already done considering the fact that it has existed prior to the transition of INS into CBP, so I'll have to look into that. Then if your research tells you that there exists no Privacy Act SORN as well as PIA on that, I will have to get back to you on that.

Mr. Beales: We would appreciate that.

Ms. Sotto: Mr. Sabo.

Mr. Sabo: Just two questions. One on, and it may be something we have to research, but the US Visa Program, as I understand it under the US VISIT Program in terms of the privacy protections that it offers, if I'm not mistaken, they've made an effort to include under the Privacy Act, protections non- US citizens or others who are, I forget the other categories, citizens and those who are permanent residents under the Privacy Act, but they've extended the same rights to non-US citizens, and if that is correct, and I may be wrong, but I think I was briefed on that at another committee. If that is correct, then my question would be for consistency. Would that be a possibility or why isn't that possible under the CBP rules that you're operating under for privacy protection? The second question, comment, gets to Mr. Kennedy's point about when somebody contacts you through your process to request a correction of records, what standards do you use to identify those individuals so that you can be sure that it really is the record that you're correcting? In other words, you said earlier they just write you, and it's a very simple process. Do you require that they present notarized documentation of their name and their identity? What forms of proof do you require to establish that they are who they say they are, and how does that compare to what is happening on the parts of DHS? I guess it's a policy consistency question.

Ms. Bell: I'm not sure exactly what forms of proof we have precisely other than the signature and the letter attesting to the fact that you are who you say you are.

Mr. Beales: I think it goes to an earlier discussion about the need to look at policy consistency across DHS agencies because otherwise, you're having not necessarily equitable treatment or issues of equity necessarily. There may be efficiency and just consistency. As long as it's appropriate, there may be reasons you need stronger proofs for other purposes, like insuring your names on a list of potential terrorists.

Ms. Bell: With respect to your other question concerning the Privacy Act, it is by law that the Privacy Act only applies to certain people. Generally everybody gets the benefit of the Privacy Act because in our agency, we generally treat people who would not be protected by the Privacy Act or subject to the rights under the Privacy Act as being eligible for redress, so to speak, through the Freedom of Information Act, and so, since that allows or that is something that could be applied to everyone, we would treat or turn a request that would normally possibly come in under the Privacy Act as a Freedom of Information Act request and provide the maximum information we can under that statute.

Ms. Sotto: Thank you. I'm going to now turn to our final witness on this panel, Jennifer Barrett. Ms. Barrett is the chief privacy officer for Acxiom Corporation. She joined the company in 1974, which must be a record of some sort. Ms. Barrett is responsible for the oversight of Acxiom's global, public, policy, privacy and information practices. She provides direction for Acxiom's information use policy across all global operations. Ms. Barrett speaks frequently on privacy and customer relationship management, and she has testified numerous times before Congress. Recently she was appointed chair of the DMA's Committee on Social Responsibility, and she's a member of the executive committee of the Center for Information Policy Leadership and the Information Policy Institute. Welcome Ms. Barrett.

Ms. Barrett: Thank you. It's a pleasure to be here and to see a number of faces that I know. Let me give you two minutes on who Acxiom is for those of you that don't know much about the company because it will help frame the context of my remarks. I will also say from the beginning, I am not here to comment on what DHS is or isn't doing in this arena. What I'm here to do is to share with you a program of redress that we've had a place or that we started in 1990 and obviously has refined and matured over that period of time and maybe gives us some thoughts on how it contrasts to some of the things done in the private sector with what or already is being done in the government sector.

Acxiom is an international company. We have locations in 13 countries, so we deal in many different legal regimes and deal with this issue in all of those regimes. We have about eighty percent of our business in the US is internationally providing computer services to large companies to help them manage and understand their customers

information, and sometimes those services are in support of their own redress activities. About twenty percent of our revenue constitutes a lot of information products which are used both in the marketing arena as well as in the risk management arena, and it is that area of our business where our own redress process comes into play. We have information on virtually all consumers in the US and in some cases, in our risk management applications, it does include very sensitive information such as social security number, drivers license, date of birth and so forth. Consumers reach out to Acxiom for a variety of activities in this area, some of which are the opportunity to opt out of those marketing products if they do not wish us to license or sell their information to third parties, and that is a fairly routine and automated process. On an annual basis, we would interact with, well I think in 2004, it was in excess of 30,000 individuals over the course of the year, and the vast majority of those are consumers that either want to know what we informationally have about them or wish to opt out from those products. The process of finding out what information we have about them is a little bit more involved.

A consumer can contact us and simply opt out by going through a process that is outlined on our web. You can call us on the phone, and we'll talk you through it or a voice recording will talk you through it, or you can write us a letter. But if you wish to get access to the information you have, then we go through a series of steps to authenticate the individual is who they say they are because obviously you do not want to provide personal information, including sensitive information, to someone who is not that individual, and then we would provide them the information. On a small number of instances, the consumer will contact us either regarding a problem that they have and, typically, that had been referred to us by one of our clients because we're not using their information in the marketplace our clients are, and we encourage our clients.

If the consumer has a problem related to the information we've provided, to contact us and refer the consumer to us so we can resolve it. We use a four-step process when a consumer, after a consumer has made initial contact with us that includes again, an authentication step, a problem-identification step, a research step and a resolve step, and it's around these kind of four components that we built a process and over time, having refined and improved that process both through expansion of our business, learning what other regimes and other countries have required as well as just through the school of hard knocks. We have a department that actually reports up to the Privacy Office called Consumer Care, and we named it that and in that department, we have a consumer advocate. We named it that because part of what we're trying to convey is that this particular individual and their team is responsible for representing the consumer's protection for the rest - that is a role the rest of the company views them as having. It is not viewed as a legal role. It is viewed as really a caring, important role, and we have a saying there that our objective in dealing with consumers, particularly consumers with problems, is to treat them with kid gloves meaning we really want to try and resolve

whatever the issue is that they have. It is a one-stop shopping department where the consumer can contact us and resolve any variety of issues that they might have. The department has four main goals that I will share with you.

The first, through the authentication process, is to prevent bad guys from gaining the system, and I think with any kind of redress process, authentication is a key element. We try not to make it overly burdensome, but on the other hand, there has to be a balance. We don't use notaries or other types of external verification. We go through processes much more similar to what you would use if you went online and asked for a copy of your credit report or asked a series of questions. We have the advantage of having authentication services we sell to our clients, so we can use them ourselves for these particular purposes.

The second goal of the department is to provide reasonable and responsive action to both the consumer and the company, and I think we have a balance here. Access and redress are sometimes discussed in the absolute terms, and I think it's important to understand there has to be a balance between what is practical and reasonable for a company to do as well what the consumer would like to have happen.

And the third objective is to remove, correct or as a very last resort, to instruct the consumer with what actions they need to take to correct the information. In some cases, we are a downstream user of information, and it is not only important for the consumer for us to correct that consumer's information in our own records, but to inform the consumer where they can go to correct it because we're certainly not the only source of that information. And if they fix it with us, but they don't fix it at the original source, in some cases, they're actually wasting their time. I would like to tell you a story because I think it kind of typifies the instances that we have when we're dealing with an error, and I think it is one that you will find maybe both informative and amusing. A number of years ago, a young lady called us in a panic saying that she was receiving telephone calls and mail at her home addressed to the arsonist of the house that she had previously lived in. Now as you can well imagine, this was a little bit concerning, and we took down the information she had and didn't know the arsonist name and hers and the address and so forth and did some research into the incident.

As it turns out, yes in our records, in fact, in most of our databases, it was a gentleman who was the arsonist. His name was listed at her address, and so we did a little further research to find that not only was his name listed in her current address, but his name had been listed at her previous address which kind of gave a little bit more interest to the issue, so we followed up with her. And in most cases, these are dialogue-type activities. They're not done at arm's length. In fact, we require that we have contact information to be able to interact with the consumer because more often than not, we're not sure what the issue is and what information we will need. So we contacted the young

lady and informed her that not only was the individual's name listed at her current address, but it was listed at her previous address, and a little more of the story unfolded. As it turned out, this happened to have been a former boyfriend who had lived with her. They had broken up. He had become concerned and angry over the breakup and had burned her house down. When she had moved to her new address, she had filed with the postal service, as most of us do, a form saying that she wanted to have all of her mail forwarded, and in that form, she had checked the box saying this is a family move which, to the postal service, means move everything that comes to this address to the new address. Once we found out what the story was and were able to share with her why this was happening and how she could fix it, we actually ended up with a very loyal consumer who sent us a thank you note, not just for responding the way we had responded to her particular concern but the fact that we had helped her deal with the root of the problem as opposed to some of the symptoms. I tell this story not necessarily frequently, but I have, on a number of occasions, become the good points to the difficulty in dealing with the inaccuracies and particularly the information flows we have where we are information originates in one bullet is assumed to be correct then. There's been discussion here about accuracy and the problems of having information that is inaccurate flow through the system and be passed on, but I think it speaks to the fact that we have to kind of look at the issue of redress in a little bit of a holistic manner. If she had not gone back to the original postal service and corrected her request, she would have continued to have this problem in other areas. So the more comprehensive the approach can be to dealing with the solution, we actually fixed her data in our file and then encouraged her to go and deal with the situation upstream.

Consumers in this environment tend to be scared or frustrated. The bottom line is they're emotional, at least the ones that we typically talk to, and they don't understand the information flows that are taking place, and therefore, what they need is someone that can not only calm them down but maybe help them out. They just want the problem to be solved. They don't necessarily need to know all of the details of how the systems work. And quite often, the original symptom of the problem is not, it is not obvious or there's not a direct correlation to the root of the problem, and I think this is what creates the most frustration for consumers is when they think they know what the problem is, they go down a path of if it's a very prescribed path, it does not solve the problem, and they're really kind of left holding the bag in terms of where do I go from here. It requires a knowledgeable staff. In fact, the individuals that talk to consumers in our company have to have been with the company for a number of years. We've put them through extensive training to learn the systems and be able to really answer the kind of questions because they drive the research and resolve activity. Our individual areas of the business that have these information products are the ones that are responsible for actually making the corrections. And I think what you find, and there have been some comments and some

references to this previously, that over time the kinds of complaints that you get, the kinds of problems and data inaccuracies that you identify through this process are fabulous learning tools, and it's extremely important that that knowledge get back to the people that are developing and managing the systems. We initially put in quick fixes to deal with some of these, and I've actually had called upon, at late hours of the night, programmers to come in and manually fix files. Now it's been a few years since we did this, but in the early days, manually fixed files because we didn't have a process to correct something. We put in kind of a positive list, much like was described earlier by TSA, where you kind of override the fact that the data is wrong, so you fix it before the final decision is made. But on a quarterly basis, we share a summary of all of the kinds and categories of complaints and issues that we're dealing with with those product people, and our department actually identifies kind of a target list of system fixes that we then work with the individual product owners to implement as they make changes and upgrade and innovate the systems.

I can say today the tools we have not only to research the problem, and that requires tools as well, because if you don't have good systems with tools to look into why is the data in the state it's in, then you're really never going to get to the root of the problem, but also then to deal with the inaccuracies and correct them in as expeditious and as permanent a way, and permanency is also a component here particularly when you're receiving data from third parties where they're going to essentially request the information you have, and you have corrected that information in the interim, and it may not have gotten back to the source that requires some additional systems approaches that have to be in place. It is an irritative process.

I think that -. I can certainly say we weren't very good at it in the beginning when we first started down this path. Our goal today is that we have much, much higher consumer satisfaction, and we measure that, and we track that in relation to do consumers feel that they were dealt with in an appropriate and effective way? I won't claim we're perfect. We don't satisfy everyone's objective. In some cases, we can't. But in the vast majority, we have figured out ways to accommodate them or to direct them to the right place, and I'm happy to answer any questions you may have.

Ms. Sotto: Thank you very much, Ms. Barrett. Lance Hoffman.

Mr. Lance Hoffman: Thank you. I'm interested in metrics. You commented that you looked at what happened and quarterly you reported back to your customers basically and said, Well, we found this, we found that, here's how we're performing this, how you could do better, is in essence what I got out of that. My question is, do you have any data you could share with us or at least give us general knowledge about in terms of the number of inquiries you process per person per unit, time or something? What I'm struck by here is the analogies, and maybe differences, between your operation and Mr.

Kennedy's operation, and this may become a question for Mr. Kennedy later on also, I'm not sure, but I'm struck by the fact that for one thing, you require a dialogue you said, where it sounds like, I wouldn't quite call a dialogue, sending in of three notarized forms or of something like that. Maybe there's a difference there. Maybe there isn't. Similarly in this case, the TSA case, there is a notarized paper basically floating around. In your case, it sounds like it's, I could be wrong but, telephone interaction or web based or a little more relatively more electronic to some extent.

Ms. Barrett: Yes. Let me answer several of those questions. First of all, the metrics one. We deal with tens of thousands of consumers every year. We do not deal with correction, data correction activities. The number is down more in the thousand or a little bit greater range, so it does allow us the opportunity to have a little bit more personalized interaction. The consumer does fill out a form. When they first request correction, we have a certain amount of information we need from them both to answer, to deal with the issue and investigate it, but also to authenticate them, and they can print that form off our web site and mail it in or we'll send them a packet of information, and they can send that in. It does require some corroborating identification. There are several things you can send in to verify that you are who you say you are. We do not require a notary. And it is more of a matter of our asking enough questions that we can correlate that this person is pretty much who they say they are. If they're not asking for access, if they're asking for correction, while we are very interested in making sure that they are who they say they are, we're also concerned that we verify that the information that they are correcting is correct, and that could be, probably, the largest challenge. We've decided, and I think this is just a company philosophy, these consumers are customers of our clients. They're not customers of Acxiom, so we don't have a direct relationship with them. But because they're customers of our clients and we care very deeply about making sure that we aren't the one that irritates a customer of one of our clients because our client is going to hear about it, we have a big incentive to really give them the kid glove treatment. And we found that some of these research and resolve activities take dozens or more man hours and effort to deal with, but if they turn into be something that is repetitive, that's when we'll put in automated processes both to do the research or to correct the data.

Mr. Lance Hoffman: Thank you.

Ms. Sotto: Thank you. David Hoffman.

Mr. David Hoffman: Ms. Barrett, thank you for being here. This question would go first to you, but then I think also to the entire panel. You mentioned a process for doing research on customer satisfaction or a satisfaction of people who've been through the redress process. I'm wondering if you and the rest of the panel could talk about to the degree that you do research into the awareness of individuals about the redress process and whether the mechanisms for communicating the redress process are effective.

Ms. Barrett: We have not done, per say, research in it, but what we have done is we have a very aggressive program to inform our clients. Because we don't deal with the consumer directly, we're a secondary referral that they need to be sure and refer any consumer to us that has a problem with any of the data we have provided. We think it works. In fact, we think it may work sometimes a little too well because sometimes the clients will refer the consumers to us about one of their problems, not one of ours, that we have to send back. But I think the challenge -. Well, with the areas, that we think that one-stop shopping is extremely important. We have a wide variety of products, over 20 different products, and rather than have the consumer deal individually with them, we would prefer the consumer to deal with one department that then fans out in our organization and deals with all of the different variations. I think the consumer is highly frustrated if they fix something in one area then have to come back three months or six months or a year later and fix the same problem in another area of what they were perceived to be the same company or maybe even the same agency.

Mr. David Hoffman: Could other members of the panel comment on that?

Ms. Bell: As I mentioned, I think the first thing we would have to do is answer the question about whether or not it's posted on the web about the Customer Satisfaction Unit. That being the case, and not readily being aware of that, I know we have a problem, so we'll have to look into that part as an initial step and see what else we can do.

Ms. Hunter: When we help a specific customer, we ask them to get back to us if their case isn't resolved, which isn't ideal, but often USCIS is the only entity that can actually solve the problem. So to the extent that it hasn't been solved in a certain amount of time, we ask them to let us know again. We understand it is not ideal, and we're working on making it a little bit better. And as we're working toward making our process a little bit more automated, we will be doing a little bit more of a public campaign to tell people more about our services as we get more sophisticated.

Mr. Kennedy: At TSA, actually we have -. In the beginning when we started redress, it was called our contact center and then they will send out some information to you, and then you fill it out and send it back in, and it was kind of like a back and forth, and what we tried to do is give people as many alternatives as we can as to where they can actually get the information that they need on how to contact us. We still do it through our contact center. We have the information posted on our web site, and also when a person is impacted and they say something at the airport, or the airline, the ticket counter, the ticket counter will tell them this is how you contact TSA as well, so we have many different ways to let people know Hey, the office of redress is out there plus in forums like this where we talk about different, about redress, but that is kind of how we get our information out there, and we talk with people about the effectiveness of our outcome. As you can kind of imagine, TSA is fairly popular right now and so if they have

a problem, they usually don't have any problems in letting us know that they're still having a problem and we still need to work on the solution. It's not perfect, but it is light years ahead of where we were.

Ms. Sotto: Thank you, Mr. Kennedy. We'll take two more questions, Jim Harper and then Joanne McNabb. Thank you.

Mr. Harper: Do you provide services to the federal government?

Ms. Barrett: Yes we do, and as a subcontractor, we have provided some services to DHS, to different divisions of DHS.

Mr. Harper: What do you make of the idea of that Privacy Act protection should apply to private data when it is used for government decision making?

Ms. Barrett: I don't know that I've studied it in any great depth. I'm somewhat familiar with the Privacy Act and the requirements on the government. I think that it should certainly not -. The current version of the Privacy Act should certainly not be used as an out to allow government agencies to use private sector in a way that's different from what they would do if they had that data themselves, how a private company would be held accountable or included in the Privacy Act, I would have to think about and get back to you.

Ms. Sotto: If you could follow up on that, we'd appreciate it. Thank you.

Ms. McNabb: In the interest of understanding the complex data flows, how did the woman with the arsonist ex-boyfriend come to you?

Ms. Barrett: She contacted one of the companies that had sent her, either called her or sent her mail, and said, Where did you get my address? And they researched it within their own company and found out that they had received a change of address from us.

Ms. McNabb: And you'd gotten it by purchasing the post office list?

Ms. Barrett: We're a licensee of the National Change of Address Service.

Ms. McNabb: So it came from the federal government?

Ms. Barrett: Actually the error came from the consumers themselves who filled out the form wrong. The data came from the government. It was an example of where we can't correct that data. I can't go back to the postal service and say, "Please correct this on behalf of this consumer." And under my license, I have to still provide that change if should someone come to us with the old address and the new address until the consumer corrects the information. But I think the important point of the story here is making sure the consumer understands that so that they can take care of the problem themselves.

Ms. Sotto: Thank you very much. I just want to ask a question along those lines. You talked about propagation of corrections throughout the system, and I think that is

such a critical piece to this puzzle because otherwise you're treating the symptom without treating the underlying problem. Can the rest of the panel comment please on how you would propagate changes throughout the system and what does that system mean to you? Does it mean your own division or a piece of the puzzle, or does it mean you're trying to propagate changes throughout DHS?

Ms. Bell: For the systems that Customs and Border Protection administers, to the extent a person comes in or asks a question, they don't know what system has the information in it. So to the extent there is a correction to be made, that correction is made to all the systems that would have the information over which we have control in our targeting tools that you saw when you visited the National Targeting Center operate on a real time basis, so they're drawing from databases as they have been corrected.

Ms. Hunter: We would have a dialogue with USCIS on ways to improve the overall system and then ultimately send them a formal recommendation to make those changes in the overall system, and to date, we have sent over 23 formal recommendations.

Mr. Kennedy: At TSA, we actually -. When we find there is erroneous information or potentially erroneous information about an individual, what we would normally do, what we do is, we actually go back to the Terrorist Screening Center who actually goes back to the nominating agency and corrects the information at the source, so we are consumers of that information, but we're not the ultimate generator of that information, and we give the information back.

Ms. Sotto: Thank you very much. I'm going to stop questions for this panel and thank this panel very much. If we have follow-up questions, may we contact you? Thank you all. We would very much appreciate your testifying today. Thank you. Before we turn to the next panel, I would like to just announce that if you are interested in speaking at the end of this session, if you're a member of the public, you need to please sign up in advance. Outside the room, there's a sign up sheet. Would the next panel please come forward? I appreciate the indulgence of this next panel for letting us run over. We have the great good fortune today of being joined by two European data protection authority representatives. We are delighted to have you and are very excited to hear your input. The first person on our panel is Peter Schaar. Mr. Schaar is the federal data protection commissioner for Germany and is also the chair of the Article 29 working party of the European Data Protection Commissioners. Mr. Schaar is the formal deputy of the Hamburg Data Protection Commission and a member of the Attendant Commission to the Modernization of Data Protection Law. Thank you very much for joining us.

Mr. Schaar: Thank you very much for the invitation. This invitation gave me the opportunity to listen to your discussions and your proceedings this morning, and it was extremely interesting for me to hear that you are dealing with the same questions, that

you have to tackle the same problems as we have, but it was very interesting to hear some new ideas, and such an advisory committee is one good idea I think to come to good solutions, so thank you very much again for the invitation. I have provided a more comprehensive presentation that was circulated, and whoever is interested can access it outside the room so I can be short. If you want to know more about the content, read it. So we have more time to discuss the really interesting issues, I want to focus to a few key issues.

First of all, the questions about the European cooperation. There are two different cooperation models within the security area. The security area is not covered completely by the European Community Law, and so every member state is more or less independent in this area. Only the cooperation procedures can be regulated by so-called framework decisions or by international agreements. And therefore, we have a completely different situation in the area of the security cooperation, the collegial and judicial cooperation from the situation in the common market. We have a kind of domestic market of products and services. Therefore, we have a general data protection directive in this area, and we have particular special data protection directive on the area of communication, electronic communication needs. So in the third pillar, the so-called third pillar of the European community, it is much more difficult to come to a free exchange of information than in the so-called first pillar, the market.

Although there's a need for better cooperation, the first way to cooperate in this area, the older approach, is to come to common information systems. That's one example is Europol, another is the Schengen information system, others are customs information systems, and there are several different other international systems. Europol is a system, a technical information system for the police institutions all over Europe or not all over Europe, in most European member states, and Schengen is also an information system. Schengen is a system or is a result that of the abolition of the internal orders within all over the European community. Therefore, there's a need to cooperate in the area of border control especially, and the Schengen system is the key system to exchange information about such persons and also other stolen products, cars and so on. And there is preparation for an enlargement of the scope of the Schengen systems to biometrical means and other new features. Many institutions have access to Schengen system, and the figure of the institution should be, following the plan of the government should be enlarged further.

Another form of cooperation is direct cooperation between the police institutions, that this is on the focus of the European governments now. They key word in this area is the availability principle. That means that every police of a member state should have the same rights as the local police if they want to know data about persons or personal data stored in another's members state, so the same idea or similar idea as in the domestic

market. I say it's a kind of domestic market of security institutions, so there is no doubt that there must be, in the era of terrorism, better cooperation between the different polices and the member states and not only in Europe. We need also a better exchange with third countries, especially with the US, but there must be also guarantees, guarantees for the privacy. And so far as we are concerned, there must be other guarantees too to other fundamental rights. We had a recent discussion on this, but I will not mention this today and that this goes beyond my charge or my competences. So while we are discussing in Europe about data protection regime for the third pillar, that means that as in the first pillar, we need also a data protection or an adequate high level data protection in the area of police and justice.

So recently the European commission has released a draft framework decision on this question. And for me, there is a very, very close relationship between the availability principle on the one hand and the adequate level of data protection on the other hand. And so we will discuss with the commission, with the European parliament as well as with the counsel, this approach. I hope it will be, remain a package. I'm not sure because the police institutions are not so interested in the adoption of this data protection regulation as they are interested in the adoption of the availability principle. So I come to the second main issue that's the question of the transfer of personal data to third countries, especially to the US.

As you know, in the first pillar, the European commission has to adopt so-called adequacy decisions. That will be the issue we will discuss tomorrow with the FTC on a specialized seminar on the safe harbor. Well, on the third pillar we have not such instruments until today, but this question has to be addressed, too. In this regulation for the third pillar, from my point of view, it should be addressed because there should be the kind of formalized process of transfer of personal data to third countries. We have a need to guarantee an adequate level of data protection in the third countries on the area of police and justice too. That means that there have to be guarantees, and I was very interested to learn today that there are two main points or two main issues not addressed by the US Privacy Act.

First of all, that only US residents are protected, and second is that the access, the governmental access of two commercial private databases is not covered by the US Data Protection Act. That is for me, it's a problem because from European view, the fundamental rights of the European citizens have to be protected. That means that although if a European person travels to the US, he or she should be subject to the protection of the US law, also the Data Protection law, and also, if databases driven by private companies containing also data of European citizens can be accessed by the US police or other governmental bodies, this should be also be only possible under the privacy protection regime.

Therefore, I see these two main problems. There are many opportunities or different ways to protect data, personal data. Also in this area, one would be the extension of the US Data Protection Act. Another opportunity would be special agreements. We know the discussion about the PNR agreement, there are undertakings. And the first speaker today of the US, of the DHS policy department pointed out, correctly, that we had had an inspection and review on PNR and substance. We see that the US complied with the agreement and with the, with their own undertakings. So it could be one solution, but I question whether it would be the best solution. I'm not so sure. I have two reasons. As you know, the PNR agreement is not so stable. The European court will come to a decision on this issue. The attorney general at the European court has said that there is no basis for European institutions to come to an agreement that we're not concerned against the level of data protection. It was the general question whether European law can cover the transfer of data, of private databases, to the US. And if the court decides that the attorney general proposes, then we have a problem.

So I cannot say whether we would be, what would be the solution of perhaps there should be many, many, many bilateral agreements. It would be a crazy way. I think another way would be a general multilateral agreement that guarantees or would guarantee an adequate level of data protection. So let me conclude. I think that if we travel or we come to the US as Europeans, we have to accept that the privacy idea comes from the US. It doesn't come from Europe. And in general, we have the same, we follow the same principles. We have different legislatory systems, we have different regulations, but I think we can learn of each other, and then we should improve the general level of data protection and interlinked and interconnected world. Thank you.

Ms. Sotto: Thank you very much. We very much appreciate your remarks. Questions? Joe Alhadeff.

Mr. Alhadeff: Thank you, and let me join the chair in thanking you for coming and providing a very useful insight into these issues, and right now especially with the third pillar suggestions being made for a framework of data protection within the third pillar. As you noticed in our discussions, one of the things we're trying to deal with as a committee is the places where not how it works in the third pillar by itself or how it works in the first pillar by itself, but how it works when the third pillar and the first pillar kind of become one because in looking at the antiterrorist information, there's just somehow a need for information to be sourced from what worked traditionally for first pillar organizations. And clearly in Europe, the data retention issue has clearly been one that married the first pillar and the third pillar perhaps a bit prematurely before the frameworks were all developed. But to the extent you could provide some guidance or some, shed some light on how that specific issue is being dealt in Europe, that would be very useful.

Mr. Schaar: Well, it's a big problem in Europe because we have this regime, this distinction of the pillars. The pillar regime of the European Union should disappear with the European Constitution, but you know about the problems with the European Constitution. It was rejected in France and in the Netherlands, and so I am not sure whether we will have a European common constitution in the next five years or so. I hope we will, but I'm not so sure. Therefore, we have to deal with the actual or the recent system or the pillar system.

So you mentioned the data retention issue. I will not go into the details today, but also the question whether this falls under the first or the third pillar was a question, and it is not answered yet, not really answered. The council of ministers said, oh, we are competent for this. That's because it's a third pillar issue, that's true. It's a question of the cooperation between the police and the justice and all over Europe, but the first pillar institutions say also, we are competent. So the compromise found in European parliament would be one way because also, the council of ministers has to agree with if there is no agreement with the council of ministers, this will not be adopted, only by a simple majority. So we deal with this. We say, as data protection authorities, and also the European parliament says if there are regulations concerning fundamental rights, independent whether it's only covered formally by the third pillar, those regulations, those limitations should be, must have a legal basis and a parliamentary decision.

That is a common tradition in Europe and, I think, in the US too. The council of ministers is only a governmental body, and therefore, they have their own interest, and the national parliaments can supervise them, but they cannot give them any directions. So I think the best way would be that the European parliament and the council come together to common solutions.

Ms. Sotto: Thank you. I have a question. We, of course, are very well aware of the right of access and the right of rectification in Europe with respect to data. Could you talk a little bit about those rights with respect to data maintained by law enforcement officials throughout Europe and then how changes, if they are permitted to be made, are disseminated throughout the system?

Mr. Schaar: Yes. Well, there are different solutions in the different member states of the European Union, in Germany, and in the most European countries. The individual has the right to access to his or her personal data independent whether it is stored by public or private bodies including police and also intelligence services, but there are some special regulations of course. And if there is law enforcement data, the law enforcement agency has the right to say to reject a request for access to information without giving any detailed explanation to the individual. But in this case in Germany, the data protection commissioner gets the whole answer.

So we can get, we can supervise whether the data is stored in a correct and legal way or not, but we have not the right to inform the individual. If there is no, if it is not agreed by the law enforcement agency in France, for example, there is no such right to access to personal data stored by the police. In Europol, we have special regulations. Perhaps my colleague can say more about this. And so under the proposed, the draft, of the framework decision on the data protection in the third pillar also contains the right of access to data stored by the third pillar institutions.

Ms. Sotto: If a law enforcement official chooses to, if they have the discretion to say just to a very small percentage of individuals who ask to have access, No, we're not providing your access, wouldn't that tip off those individuals that there is some ongoing investigation?

Mr. Schaar: Yes. And therefore, the law enforcement agency not only says no in cases where there is an ongoing investigation, they say no in other cases too, not in all cases but in more cases than there are investigations.

Ms. Sotto: More questions? John Sabo.

Mr. Sabo: Just a quick question. As you see increased data flows as the framework gets fleshed out in actual agreements and structures, what are your thoughts about compliance, establishing that the various entities are conforming to the laws and the agreements? That always has seemed to be a weak point in any privacy regime, the ability to enforce the agreements. What are your thoughts about the directions you're going in Europe?

Mr. Schaar: I think, in general, there's a good compliance with the data protection regulations, also in the area of police and justice. Perhaps it is better than in the private sector. The question is -- what are the procedures? And in Germany, we have internal privacy offices like in the US. The Privacy Office of DHS additional to the independent data protection commissioners who are supervising, in an external way, the data processing. That is one solution. Not all member states follow this solution. A second is notification. Also in the public sector, that means if there is no privacy officer in a special office, many administrations are obliged to notify the data protection commissioner about their data processing. And there are different ways on the European level to supervise data, the data be in compliance with data protection laws. There is a joint supervisory authority for Europe, in Schengen and for customs, too. And this joint supervisory authority deals with complaints as well as it carries out its own audits, data protection audits.

Ms. Sotto: Thank you very much. Mr. Purcell.

Mr. Purcell: I would like to hear your comments on what we all fear of a possible medical pandemic regarding avian influenza, and our cultures may disagree on some

points of privacy, but we all agree that medical privacy and health information is sensitive data and deserves high levels of protection. This will be challenged in the case of a large-scale global medical emergency or a pandemic. How is that going to play out where we seem to be behind the policy curve in this regard?

Mr. Schaar: So far as I remember, we didn't address this item on the European level. We asked our German authority - that is in charge of things - about the processing of personal data and they answered, and until now they don't process any personal data. So we didn't deal with that until now. I know that also some supervisory authorities for farms, for example, are involved in these questions, and they collect also the data of the owners of the farms, especially if the new influenza, the chicken influenza or bird influenza or so. It has its very own translation so, but I think we have to address this question on the European level too, and it also covers diseases like HIV. So the question is how we deal with new dangers, and what about challenges in this area? I see it, and I will address it. We deal with health records in general, but under other aspects, especially how to deal with electronic health records especially.

Mr. Purcell: One follow-up if I may. It seems that this will collide with the passenger name record issues that are currently in front of us as global travel facilitates the spread of disease carriers or potential disease carriers, so what happens when passenger name records start carrying sensitive medical conditions?

Mr. Schaar: That's true. There are two questions referring to the name records, the passenger name records, the first is where the passenger is from. Does he come from an area with actual dangerous or recent cases of influenza? That might be the first. The second would be is he a high-risk passenger? Like the terrorist assessment, you can say, Oh well. If he is a farmer, it might be that he is a high-risk person and he has to be screened in another way than the other passengers. So the authority needs information about the profession. It might be a problem yes, of course. We didn't address this until now.

Ms. Sotto: Okay. If there are no other questions for Mr. Schaar – oh - Mr. Palmer.

Mr. Palmer: Just very quick. I'll probably show my ignorance of recent decisions. At one point, there was a ruling in Germany or Europe, I'm not sure which, that said basically we have these rules about protecting data, and by golly, if you want to play with us, you're going to protect the data the same way, and it was some noise I heard about the data will not be allowed to be shared with countries or corporations if you don't protect the data the right way. Is this just a nightmare that I had, or is this really true? And if it is true, is it actually going to happen, especially given the comments you made earlier about what you learned today?

Ms. Sotto: I think that's too broad a question.

Mr. Schaar: There are such decisions on the national level as far as I'm informed. And in general, the question, it's a question of judicial and police cooperation between the member states of the European Union and other states especially with the US, we have such questions. I think, if there are guarantees, that the data are used in an appropriate way, there are no problems. And so far as I'm informed, the European police institutions give data to the US. And we have special agreements, for example, Europol or especially Europol. On Europol, there is an agreement with the US, and there are some definitions what is adequate level of data protection and limitations and so on. That might be a way. And so I see that data of Europol or from Europol flows to the US, but also, the US doesn't give all information to the European member states, not because of reservations about not adequate level of data protection, there are other reasons.

Ms. Sotto: Thank you very, very much. We may have some follow-up questions for you, but thank you Mr. Schaar. Our next speaker is Agustin Puente. Mr. Puente is head of the legal department of the Spanish Data Protection Authority. Thank you so much for joining us.

Mr. Puente: Thank you. First of all, I want to thank you on behalf of the head of the Spanish Data Protection Agency who wanted to participate in this committee, but some other obligations have made it impossible. And second, I want to thank the committee for allowing us to participate in this issue. I've listened very carefully to Mr. Schaar's presentation, and I want to try to compliment what he has said with some other views, especially from the practical point of view, some problems we have made at the Spanish DPA and also at the European level.

Basically, I think that the cross border cooperation could be fulfilled by two ways. First of all, getting improving cooperation between the different states and second, trying to solve practical situations. The first is because, taking into account what Mr. Palmer has previously asked and what Mr. Schaar has said, the region of privacy, of the consideration of privacy as a right of the citizens of the United States are not different views, I think, that could be - they are different approaches but not different considerations about the fundamental right to privacy in the United States and Europe because the United States is the original of that fundamental right. And on the other hand, the original data protection principles as they are considered today, the data limitation purpose, the nationality, transparency information rights are not included in a pure European instrument but in the guidelines of the OECD that were previous to any European approach to the data protection. And so most of the European countries and of course, the United States, are part of the OECD and under those principles, are included in the UN guidelines of 1990.

So I think one of the most important ways to solve the problems that could appear in the cross-border cooperation, try to make the data protection principles achieve the

same data protection principles, maybe not with the same approach but just the same principles to be achieved by all of the countries. The cooperation is gotten by the different ways Mr. Schaar has said. Mr. Schaar is like, for instance, the agreements between the Europol and Schengen with some third countries and of course, the United States and also in Spain. We are trying to get that new approach with the lent in American countries, one of the last actions of the Spanish Data Protection Agency was to cooperate with Latin-American countries and create a so-called inter- American data protection network to achieve the same level of protection, maybe three different instruments, but achieve the same data protection. The second issue that is important dealing with this cross border cooperation could be the practical approaches and practical solution and problems we have found in the Data Protection Agency in Spain.

First of all, I wanted to talk about something similar to the PNR and the access to the passenger name records that is not the same regulation in Spain, but something similar. As you probably know, there is a European directive of 2004 which obliged the transporters to facilitate several data to the customs authorities in Spain in order to prevent the illegal immigration. In Spain, there was a previous solution previous to the directive in 2003. The Spanish home office, the minister of interior, wanted to get an agreement with the most important airlines in order to oblige them to facilitate several data, not all of the PNR because all of, as you know, one of the problems of the PNR is the large number of data are included in it and also included in the fact that some of the codes include sensitive data. Well, this agreement in the previous version of the agreement, includes a provision in which the airlines should give all the information of all of the passengers that are going to take flights 40 hours before departing to the ministry of interior in Spain. This was submitted to the opinion of the Spanish agency, and we'll have several meetings with the Spanish Minister of Interior.

And finally, we got a solution trying to convince the Spanish authorities that the proportionality and the accuracy of the data that are going to take from the airlines would be even, would even make, be made, be even made easier as a way to pursue the thoroughism and the immigration issue, which is becoming a very hot issue in Spain. The solution was that the airlines will give the data regarding the number of passengers that don't take the round trip. And in several specific selected routes, due to the large number, the large volume of people who are coming to Spain or due to the large number of immigrants coming from these routes, the airlines would provide the data of the name of the passenger, the number of passport and the date of birth, only those data.

But only from those routes that would be most important taking into account the volume of immigration coming from this or even the number of cases that have been investigated about the traffic of human beings from some countries in South America and some other in the ex-Soviet Union. And so I think with only those data and only those

routes, the solution and the investigation could be focused on the most important, the most important aspects and the cases in which it's most probable to find several cases of illegal immigration, the human being trafficking, et cetera.

For instance, I think it is easier to investigate these several cases coming from some countries not investigating from illegal immigration those flights coming from the United States from Washington. It's easier to find out some criminal evidence in a flight coming from some countries than in a flight coming from Washington, for instance. Maybe I'm not right, but what we have tried to do is to balance the data protection principles and the purposes why the police are investigating the situation. Similar solutions we have been trying to achieve with some other cases. For instance, with the financing of terrorism because in Spain, for a long time since the sixties, it is a very hot issue, a very important issue, and it's necessary to investigate those situations. And we are cooperating all the time with the Spanish units of the security forces that are in charge of pursuing the money laundering and financing terrorism. The most rest of the problem we have found is to find out the list of people that could be involved in these types of activities in order to facilitate the operations.

And once again, we have thought that the principle and the proportionality would be very important because for instance, one list of political disposed people, persons could be not realistic if we include, if we don't take into account the situation of it's country, for instance. So we are trying to find out how to establish this kind of list and how to cooperate with the police forces of other countries. Another question we are trying now to get solutions is with the financial fraud, like phishing or credit card fraud.

We have an agreement with the Spanish police in order to facilitate and also to take the mechanisms given by the European union in order to get the cooperation of other data protection agencies or anti-spam agencies to facilitate that there will be no phishing, you know, the using of internet in order to take the identification of the bank customers. And the last point in which the cross-border cooperation could be very interesting from the Spanish point of view is precisely the cooperation with the United States of American and particularly, with the Federal Trade Commission.

In February of this year, we signed a memorandum of understanding with the Federal Trade Commission in order to prevent the spam and other activities that could be also criminal offenses through the internet, not only trying to give information to each other or to train people from both agencies, but what is very important in order to facilitate or to give the most evidence, the most possible evidence to cooperate in the situation in the cases in both countries and the mutual assistance in our investigation. And also in the field of internet and spam, it is also important to mention the plan that started in October of last year in which a lot of different agencies of different countries, and also the private sector, are trying to get solutions to solve not only the spam problems

but also those problems related with the internet because the situation of the internet requires the cooperation of enforcement agencies, civil and criminal authorities and also the private sector.

So this plan is trying to get a solution in that way. The first action that was adopted was to prevent this, the spam which some people use your computer to make a spam trying to get a compromised position and was drafted a letter to be sent to the internet service providers in order to ask them to cut off the connection to those customers that are proved to use these devices. Basically, I wanted to explain several cases. I think what is most important in this meeting is to solve the problems that have been raised and could be raised in the following minutes, so I'm open to your questions, and thank you.

Ms. Sotto: Thank you very much. Mr. Barquin.

Mr. Barquin: I wanted to ask a slightly different tact on the cross border issues, and that is one that we face here in the US in terms of information sharing between levels of government, federal, state, local, and while many of the issues have been technical, and in other cases they have been in some cases even statutory, but I would like to get a sense of in Spain across the, or in Spain or in Germany, do you have similar issues, or do you have a data protection framework that would facilitate?

Mr. Puente: I think it is easier in Spain than in Germany. In Spain, there are basically one state the data protection agency which takes care of any data processing made by the private sector, and they're only in three autonomous communities. There are three data protection authorities that they are in charge of enforcement related to the databases of this autonomous administration. So it is easier. Most of the principles are set out by the law and are enforced by the Spanish Data Protection Agency.

I think the situation in Spain, the situation in one country is easier than in the bilateral relationship even into within the European union and of course, in the relationship between different countries because the legal framework in Spain is the same for any autonomous community and from the state administration.

So this regime sets out the guidelines for the exchange of personal data, and as these guidelines are similar in the case of the security forces, they are similar because all of the security forces are included in one general act of the police and security forces. So in that case, the Spanish law provides that it is possible to exchange this information in the framework of a concrete police investigation. What I mean is, the police forces can process the data in two different ways. For the police investigation, in this field of police investigation, it is possible to exchange the information, and it is also possible to process data without giving the right of access. As Mr. Schaar said before, what is possible is that the data subject can come to the Spanish Data Protection Agency, and we can study. We can contact with the police and study the case, and we only inform the data subject. There

is no problem in the processing of data. And if there is a problem in the processing of data, we will tell the police to consult the data to rectify the data, but the data subject will only be informed. There is no problem with the processing of this personal data. I also remember the question in the previous round table.

Mr. Schaar: I can confirm that, in Germany, we have this more difficult situation. We are a federal state, and our constitution says, more or less, exactly what is in the competence of the lander, the states and what is in the federation with one federal data protection law covering the private sector and the public sector so far. If the public sector, the police especially, is concerned this is covered by the landerlLaw, and on the federal level, we have on the federal level not only general data protection laws, but we have also sector-specific data protection provisions.

For the police sector, in all landers we have specific laws that define the competences of the lander polices to store data for their own purposes, especially for preventing crimes. So there are differences, and I can say I can inform you about one big problem, a huge problem nobody can understand really, and it is not well understandable system that's after 9/11. As you know, many of the terrorists were so-called sleepers, and they were based, some of them were based in Hamburg. That was at the time when I was a deputy data protection commissioner in Hamburg. It was not the best because we had to decide whether the police or we have to give advice to the Senate, the Hamburg Senate, on the question whether the police should carry out so-called rastafandung.

I cannot translate exactly. It is a kind of pattern matching, putting together private databases, public databases and searching for some patterns like you discussed in the previous discussion on data mining. So all landers carried out rastafandung, but the legal provisions are completely different, and some lander, it was not allowed to use specific data for such kind of search. In two landers, there were no right for the police to carry out rastafandung, and the judge has to accept and others, the head of the police had to give the order.

Well, there is a need for harmonization, but it is very difficult, as you know, to come together on a federal level with 16 lander parliaments and 16 governments and 1 federal government, and every federal minister of interior wants to improve the situation in his way. We have a German FBI, the BKA, that has no rights on the prevention, and it coordinates, in fact, the rastafandung, but there is no such provision or right for parliaments to carry out rastafandung. So we have this difference. We have also one thing that I welcome that's on another area of the police cooperation. In the federation, we say that not every data, every policeman, in the village can collect, should be share with all police institutions all over Germany. So there should be relevance assessment, and only those data. If a person doesn't pay for public transportation, for example, and he's situated in Hamburg, the Munich Police are not obliged to notice data. But if a person

commits a serious crime, this data must be shared. And my wish would be that under the regime of availability, this relevance principle should be transposed on the European level, but I don't see it until now.

Ms. Sotto: Thank you so much. Mr. Sabo.

Mr. Sabo: Just a question, and I think you both touched on this to some degree, but the fact that in the United States, we don't have, for example, in DHS, the Privacy Officer is appointed under the law, but the Privacy Officer is not completely independent from the agency. The Privacy Officer reports to the secretary of Homeland Security. And in many other agencies, there is no such privacy officer whereas the European model, you have DPA, you have data protection commissioners and you have much more independence. Has that been a barrier in reaching agreement with the US government on sharing data? If it has been a barrier, to what degree, and is it something that can be overcome, or do you see long- term problems as long as there is this difference in the independence of the data protection privacy officer model?

Mr. Schaar: Well, I think it is a difficulty to come to an adequate level and to an adequate decision. We have some key issues to define whether there is an adequate privacy level or not, and the independent supervision is one of these key principles. Therefore, a kind of independency or different ways to guarantee this independency, organizational and functional independence of privacy supervision would be one prerequisite for such adequacy decision. Therefore, I agree with you that this is a problem.

Mr. Puente: Only to complete that the presentation this is one question we have been studying in the Latin American network, I told you before, and we have been after studying the documents provided by Article 29 working parties. It's a very important document of 1998 which tried to explain the requirements to get the adequacy, and they are substantial. These principles and those principles could be included in law and in agreements and other places, and the second is the authority, but I think that this document of 1998, they said that should be independent, but this independency doesn't mean one unique solution is what Mr. Schaar has said. It could be part of, it could be included. For instance, in some countries there have been adequacy decisions, not countries with adequacy decisions, but some European countries, the data protection officer is not appointed by the parliament but by the ministry of justice, for instance, or of other ministers or is a part of the public administration government somehow.

And in those cases, the independency could be considered, for instance, the data protection office, the data protection commissioner cannot be removed from his side in a period of time, for instance, because, well in Spain it's a different proceeding, but the president of the Data Protection Office or agency cannot be moved in the period of four years. He is appointed and cannot be moved. For instance, this data protection president

of the Data Protection Agency was appointed by the previous government. There were elections two years, almost two years ago. There is the opposite political party now, but he has been not moved. This is some kind of independency. So there are different ways to get the independency and maybe even the data protection officers in the public administration could be a way to get this independency or this adequacy that is important to study it's case, but it could also be possible without a data protection and enforcement agency, could be possible to have commissioner ombudsman, et cetera.

Mr. Sabo: Has an issue been discussed at very senior levels with the US government in terms of what you would be looking for for adequacy and independence, or is it just something that has been discussed in the working party in the EU?

Mr. Schaar: Well, we don't know what is discussed on this top level. I think it is one problem, and it was one item that was addressed in the negotiations between the European commission and the US government on the PER as well as on Safe Harbor, and Safe Harbor, we have got a solution by a kind of contractual guarantee that there should be a supervision by functional independent institutions but not governmental institutions. But on the PER issue, that was very, very difficult to come to a solution, and that is one question we discussed. We still discuss when we ask ourselves about adequate and appropriate way to protect the data of European citizens.

Ms. Sotto: Thank you. Mr. Alhadeff.

Mr. Alhadeff: Thank you. I wanted to go back to the second point that Mr. Puente had raised, and in that point he talked about -. In the first point, he talked about the OECD principles as kind of the basis, and I assume they're the basis not only of the first pillar but also to a large extent of the third pillar framework that is being developed. But in your second point, you referred to the concept of a balancing that is done when you start applying the principles, and I was wondering, is there a difference in the balancing of the first pillar and the third pillar because perhaps the interest of the state are at a greater level in that balancing, or is it the same balancing where the factor is considered the same way? Because one of the things we're gauging in this committee is attempting to deal with issues where you're dealing with privacy policies that companies have, the privacy practices of the government and the protections under the Privacy Act and how you make those things come together. So it would be interesting to find out, in the European experience, whether the balancing in the third pillar is the same as the balancing in the first pillar or if it is very contextually driven.

Mr. Puente: It is a personal opinion. I think the balancing should depart from the same principles, but that should be balanced with the data protection principle, of the data protection principles is different in the first pillar and the third pillar because the first pillar with this balance, the commercial legitimate but commercial interest and in the third pillar, what is balanced is the security. Of course the balance is different, but departing

from necessity to respect the basic data protection principles that were included in this document, I told you before, the working party number 12 from 1998 departs from the OECD. The basis, the core principles, are in the OECD guidelines.

In any case, I think those principles should be respected, but in some cases even the directive and even the conventions of Europe or Schengen and even the national laws admits that those principles could be not always applied to say somehow, for instance, the directive says it is possible not to, it is possible and it is logical not to inform the data subject he's being investigated by the police because he's being investigated for a criminal offense. So it's logical not to inform him, but if there is no concrete investigation against some people, and you are trying to, and you are obtaining data to decide to whom the investigation should be addressed, maybe in that case, you should inform the data subject that is what happens with the PER. You should inform the data subject because you are only getting information on who is coming to the United States, not who coming from the United States should be investigated.

So I think the balance should be different in the first pillar and the third pillar, but the principles should be respected, and if you don't apply all the principles, it should be on a very, very serious base. In Spain, the only case in domestic law that in which the data subject could not be informed is in a police investigation, but when it is addressed to him, not to obtain data or a potential suspect's. We had the problem with potential suspects a few years ago because the Spanish police didn't process the data of people who have been accused, in the United Kingdom, as a rapist, and this one came to Spain with another name and killed two young ladies, and there was a big criticism against the police for not processing the data of a potential suspect. And what the Spanish authorities, not only the data protection office, considered was that it was most important not to process the data of a potential suspect's that to get some kind of suspicion over a large number, a larger number of people. I don't know if I have explained it. I want to apologize for my way to express because this is not my language. I'm sorry.

Mr. Schaar: May I add something from the German side? I see a different regulatory regime in the area of commerce of commercial data processing and data processing by the government.

If so far as the commercial sector is concerned, in general, that's a question of contracts between private persons and companies or private persons and private persons. So you are free to come to an agreement, and this agreement should be fair, and we, as data protection authorities, supervise whether this balancing is carried out in an appropriate way. If there is a big company providing the servers and one individual, that is not a balance of powers, and data protection law should prevent the person, the individual as he is a consumer or an employee from an inappropriate way of data processing. That is a protection idea. If the government processes data, this is a question

that concerns fundamental rights like in the US, that's the same approach, state, individual. Therefore, there must be a very clear legal basis for every data processing. That's it.

So and the difference is that in the field of the private economy, that there must be a case by case decision, that there is not so specific law on the governmental area. There must be such very specific law, and the problem is that, under the threat of terrorism, the political debate, and also the decisions of parliaments and governments, go very far, and they are cutting data protection rights of other individual rights. And therefore, it can be only corrected by the constitutional courts, and the German constitutional court protected privacy several times recently. And the constitutional court decided for example, that there should not be a very wide competence for the police to wire tap persons without any concrete suspicion. There was in one lander law very, very wide competence, and the constitutional court said - this is unconstitutional. So we get much support by the courts as data protection officers or data protection commissioners, and we see that we have to also counterbalance the security approach and the public discussion. Therefore, I am independent, and I have some arguments with my minister of interior, but I can have this argument because I am independent. I am elected by the German parliament. I was nominated by the government, but I'm elected for five years, and I am an independent body or independent person. So that is the difference between the private sector and the public sector.

Ms. Sotto: Well, thank you so very much. We are honored to have you here and know how valuable your time is. I think it is critical for us, and well understand how critical it is, to understand the place of the United States in the global context. And unfortunately, we've learned the hard way that terrorists don't stop at our borders. So we need to understand how data also can flow through our border in a way that accommodates your needs as well as the needs of national security in protecting the security of Americans within the United States, so thank you so much. We will not seek to sacrifice privacy ever in that context, and we are here to make sure that it is not sacrificed. We appreciate your presence. Thank you again.

Mr. Scar: Thank you from my side too, and we are -. It's also our task to protect the privacy of US citizens in Europe.

Mr. Puente: And also to try to protect the privacy of US citizens, European citizens, and also to prevent terrorist attacks, of course.

Ms. Sotto: That is first and foremost. Thank you. We have not had anybody sign up for public comments, but we are delighted to take them. If you're interested in addressing this committee, please do. Step up to the microphone, and we will be glad to hear from you. Please. Voice: My name is Dr. Ally Eyeball. I have a private company I own for decision making. He made a very remarkable comment that surprised me that

OECD came up with criteria, a set of criteria. This is 1980, twenty-some years that defines according to all nations participating, including the United States, what is record sensitivity means criteria to define these different approach. You define the criteria. You prioritize the criteria, and you score the records what is private and what is sensitive, and you build a portfolio, and we did that. Our company did that, built these criteria, Mackle, and I'm really sorry to see that I was not here today, had a different approach as well. It is not looking at data. Mackle came up with a criteria to define who is a terrorist and a scale to score people. So you look at Obama Bin Laden. You look at me, and you say, He's Egyptian, but he's educated in the United States, he doesn't score that much here. He scores, and I did that for myself compared with Obama Bin Laden that the terrorist had -. These problems have been solved, and I'm really surprised that you guys have not looked into this.

Ms. Sotto: Thank you very much. We will take all comments under advisement. Other comments or questions? [No response].

Ms. Sotto: Okay, then we will adjourn. But before we adjourn, I would like to thank the Privacy Office staff. I would like to, especially, thank Becky Richards who has worked through thick and thin over the last couple of days and is expecting a baby any moment. Thank you very, very much. And Toby, we look forward to working with you. And thank you so much, Maureen. If you would like to file comments in writing, please do so on our web site. The web site is: www.dhs.gov/privacy. You can offer comments, suggestions or questions through that web site. I will officially close the meeting. May I have a motion please? Mr. Alhadeff.

Mr. Barquin: Second.

Ms. Sotto: We are adjourned. Thank you very much. [Whereupon the meeting adjourned at 4:15 p.m.].